Irreducible Polynomials for Primes

Tomás Feder[*] Carlos Subi[†]

Abstract

Let $p(x)$ be a polynomial with integer coefficients in $\{0,1\}$. We show that if $p(2)$ is prime then $p(x)$ is irreducible over the rationals. In other words, if $a_n a_{n-1} \cdots a_1 a_0$ is a prime number written in binary, so that each a_j is in $\{0,1\}$, then the polynomial $p(x) = \sum_j a_j x^j$ is irreducible over the rationals. More generally, if $p(a)$ is prime for some integer $a \geq 2$ then $p(x)$ is irreducible over the rationals. We infer this result from a more general one regarding complex roots of polynomials $p(x)$ of the stated form.

1 Results and Proofs

A polynomial $p(x)$ with integer (rational) coefficients is *irreducible* over the integers (rationals) if it is not possible to decompose $p(x)$ as $p(x) = q(x)r(x)$, where $q(x), r(x)$ are polynomials of degree at least 1 over the integers (rationals). A polynomial $p(x)$ is *monic* if the coefficient of the highest power of x in $p(x)$ is 1.

It is well known that a monic polynomial $p(x)$ with integer coefficients is irreducible over the rationals if and only if $p(x)$ is irreducible over the integers. Notice that if a monic polynomial $p(x)$ with integer coefficients can be written as $p(x) = q(x)r(x)$, then $q(x), r(x)$ or $-q(x), -r(x)$ are monic. So we shall assume here without loss of generality that $q(x), r(x)$ are monic with integer coefficients. Our main result in this note is the following.

Theorem 1 *Let $p(x)$ be a polynomial with integer coefficients in $\{0,1\}$. If $p(2)$ is prime then $p(x)$ is irreducible over the rationals. More generally, if $p(a)$ is prime for some integer $a \geq 2$ then $p(x)$ is irreducible over the rationals.*

Theorem 1 follows from the following theorem.

Theorem 2 *Let $p(x)$ be a polynomial with integer coefficients in $\{0,1\}$. If $p(x)$ is not irreducible over the rationals, so that $p(x) = q(x)r(x)$ with $q(x), r(x)$ monic with integer coefficients and of degree at least 1, then $q(a) \geq a$ and $r(a) \geq a$ for every integer $a \geq 0$.*

Proof. (of Theorem 1 from Theorem 2) If $p(a)$ for integer $a \geq 2$ is a prime number as in Theorem 1, then writing $p(a) = q(a)r(a)$ gives $q(a) = \pm 1$ or $r(a) = \pm 1$, contrary to Theorem 2. $\square$

Theorem 2 follows from the following lemma and its corollary.

[*]268 Waverley Street, Palo Alto, CA 94301. Email: tomas@theory.stanford.edu
[†]Email: carlos.subi@hotmail.com

Lemma 1 *Let $p(x)$ be a polynomial with integer coefficients in $\{0, 1\}$ and $p(0) = 1$ Let $v = |v|e^{i\alpha}$ be a complex root of $p(x)$ with $Im(v) \geq 0$, so that $0 \leq \alpha \leq \pi$. If $\alpha \leq \pi/k$ for an integer $k \geq 1$, letting u be the positive root of $1/x^r = 1 - 1/x$ (so that $1/u$ is the positive root of $x^r = 1 - x$), where $r = \lfloor (k/2) + 1 \rfloor$, we have that $1/u < |v| < u$.*

Proof. Let $p(x) = \sum_{0 \leq j \leq n} a_j x^j$ with $a_j \in \{0, 1\}$ and $a_n = a_0 = 1$. Suppose $|v| < 1$ and $\alpha \leq \pi/k$. Writing $p(v) = 1 + a_1 v + a_2 v^2 + \cdots$, we note that the first few terms $a_j v^j, j \geq 1$ have a nonnegative real part. This holds more specifically for the terms with $j \leq k/2$, that is $j < r$. In order to have $p(v) = 0$, we must cancel the real part 1 with the terms having $j \geq r$. This gives

$$|v|^r + |v|^{r+1} + \cdots > 1$$

$$|v|^r/(1 - |v|) > 1$$

$$|v|^r > 1 - |v|$$

$$|v| > 1/u$$

as desired. Similarly, suppose $|v| > 1$ and $\alpha \leq \pi/k$. Writing $p(v) = |v|^n(1 + a_{n-1}/v + a_{n-2}/v^2 + \cdots$, we note that the first few terms $a_{n-j}/v^j, j \geq 1$ have a nonnegative real part. This holds more specifically for the terms with $j \leq k/2$, that is $j < r$. In order to have $p(v) = 0$, we must cancel the real part 1 with the terms having $j \geq r$. This gives

$$1/|v|^r + 1/|v|^{r+1} + \cdots > 1$$

$$(1/|v|^r)/(1 - 1/|v|) > 1$$

$$1/|v|^r > 1 - 1/|v|$$

$$|v| < u$$

as desired. □

The following corollary completes the proof of Theorem 2 and therefore of Theorem 1.

Corollary 1 *Let $p(x)$ be a polynomial with integer coefficients in $\{0, 1\}$ such that $p(0) = 1$. Let $v = |v|e^{i\alpha}$ be a complex root of $p(x)$ with $Im(x) \geq 0$, so that $0 \leq \alpha \leq \pi$. If $\pi/2 \leq \alpha \leq \pi$, then $1/2 < |v| < 2$. If $\pi/4 \leq \alpha \leq \pi/2$, then $1/\phi < |v| < \phi$, where ϕ is the golden ratio. More generally, $Re(v) < 1.5$.*

Proof. From Lemma 1, if $\pi/2 \leq \alpha \leq \pi$, then u satisfies $1/u = 1 - 1/u$, that is $u = 2$; if $\pi/4 \leq \alpha \leq \pi/2$, then u satisfies $1/u^2 = 1 - 1/u$, or $u^2 = u + 1$, that is $u = \phi$. In the first case, the real part of v is nonpositive, therefore less than 1.5; in the second case, we have $|(1.5) + i(1.5)| = (1.5)\sqrt{2} \geq \phi$, therefore the real part of v is less than 1.5. Finally if $0 \leq \alpha \leq \pi/4$, then u satifies $1/u^3 = 1 - 1/u$, which implies $u < 1.5$, therefore the real part of v is less than 1.5. □

We finally have the following.

Proof. (of Theorem 2). We may without loss of generality assume that $q(x)$ is monic irreducible with integer coefficients. If $q(x) = x$ then $q(a) = a$ for every integer $a \geq 0$.

Otherwise $|q(0)| \geq 1$. Since $p(x)$ does not have nonnegative real roots, and $q(x)$ is positive for x large, we have that $q(a) \geq 1$ for all integer $a \geq 0$. By Corollary 1, any root v of $q(x)$ must have real part less than 1.5, so $|1-v| < |2-v|$, and more generally $|a-v| < |a+1-v|$ for all integer $a \geq 1$. If v_j are the roots of $q(x)$, then by induction on integer $a \geq 1$ we have

$$a \leq q(a) = \prod_j |a - v_j| < \prod_j |a + 1 - v_j| = q(a+1)$$

so $q(a+1) \geq a+1$, and the induction follows, completing the proof. □

As a final remark, we can tighten the bounds in Lemma 1 for roots v that are real or imaginary.

Proposition 1 *Let v be a root of $p(x)$ as in Lemma 1. If v is real, then $-\phi < v < -1/\phi$ for the golden ratio ϕ; if $v = wi$ is imaginary with $w \geq 0$, then $1/\sqrt{\phi} < w < \sqrt{\phi}$. Both bounds are tight.*

Proof. (*sketch*) The key idea is that not all terms contribute to cancelling the 1 in the proof of Lemma 1. We must take alternating odd terms for v negative so that the contribution is negative, and one out of every four terms for v imaginary so that the contribution is negative. The bounds get tighter the more terms we take. Thus for v negative and $|v| < 1$ we have instead

$$|v| + |v|^3 + |v|^5 + \cdots > 1$$
$$|v|/(1 - |v|^2) > 1$$
$$|v| > 1 - |v|^2$$
$$|v| > 1/\phi$$

while for v negative and $|v| > 1$ we have instead

$$1/|v| + 1/|v|^3 + 1/|v|^5 + \cdots > 1$$
$$(1/|v|)/(1 - 1/|v|^2) > 1$$
$$1/|v| > 1 - 1/|v|^2$$
$$|v| < \phi$$

as desired.

Similarly for $v = wi$ imaginary with $w > 0$ and $|v| < 1$ we have instead

$$|v|^2 + |v|^6 + |v|^{10} + \cdots > 1$$
$$|v|^2/(1 - |v|^4) > 1$$
$$|v|^2 > 1 - |v|^4$$
$$|v| > 1/\sqrt{\phi}$$

while for $v = wi$ imaginary with $w > 0$ and $|v| > 1$ we have instead

$$1/|v|^2 + 1/|v|^6 + 1/|v|^{10} + \cdots > 1$$

$$(1/|v|^2)/(1 - 1/|v|^2) > 4$$

$$1/|v|^2 > 1 - 1/|v|^4$$

$$|v| < \sqrt{\phi}$$

as desired. □